УДК 004.056.5 **DOI:10.30837/rt.2021.3.206.05**

О.О. КУЗНЕЦОВ, д-р техн. наук, М.О ПОЛУЯНЕНКО, канд. техн. наук,
В.О. КАТРИЧ, д-р фіз.-мат. наук, С.О. КАНДІЙ, Ю.О. ЗАЙЧЕНКО

ДОСЛІДЖЕННЯ ЕВРИСТИЧНИХ ФУНКЦІЙ ПОШУКУ НЕЛІНІЙНИХ ПІДСТАНОВОК ДЛЯ СИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Вступ

Для захисту важливої інформації зазвичай застосовуються різні технології, зокрема, механізми криптографічного перетворення [1, 2]. В основі багатьох симетричних криптоалгоритмів лежить застосування т. з. вузлів ускладнення (нелілійних таблиць заміни, S-блоків) [2 – 5]. Саме на криптографічних властивостях S-блоків базується стійкість більшості симетричних шифрів від різних криптоаналітичних атак (диференційного, лінійного, алгебраїчного та інших методів криптоаналізу) [6 – 9]. Отже аналіз нелінійних підстановок, вивчення методів їх генерації (пошуку) та дослідження криптографічних властивостей є актуальною та важливою науковою задачею.

Методи генерації вузлів заміни умовно поділяють на випадкові, алгебраїчні та евристичні [6, 10, 11].

Випадкові S-блоки забезпечують високі показники статистичної безпеки. Крім того, вони, як правило, дають захищеність від алгебраїчних методів криптоаналізу. Дійсно, якщо таблиця заміни сформована випадковим чином, тоді система алгебраїчних рівнянь, що аналітично описує підстановку, ймовірно буде надзвичайно складною. Експерименти показують, що це дійсно так. Але інші криптографічні показники випадкових S-блоків є не дуже високими. Наприклад, нелінійність (що є визначальним показником стійкості до лінійного криптоаналізу) випадкових S-блоків є значно нижчою, ніж у алгебраїчно сформованих таблиць заміни [12 – 14].

Алгебраїчні техніки формування S-блоків дозволяють отримати дуже високі показники нелінійності [9, 13, 15]. Наприклад, таблиця замін шифру AES сформована алгебраїчним способом і за нелінійністю є найвищою серед всіх відомих на сьогодні S-блоків [9]. Тобто шифр AES дійсно захищений від певних криптографічних атак. Але алгебраїчні таблиці мають дуже просту математичну конструкцію, через що шифр описується значно простішою системою алгебраїчних рівнянь [16 – 19]. Існує багато наукових робіт, присвячених цьому питанню. Фактично алгебраїчна простота S-блоку шифру AES призвела до появи нового методу алгебраїчного криптоаналізу [16]. Для забезпечення захищеності від таких атак застосовують показник алгебраїчної імунності і для S-блоку шифру AES цей показник не є високим [20].

Евристичні техніки генерації (пошуку) S-блоків зазвичай використовують випадково сформовані таблиці заміни і шляхом поступового ітераційного оновлення їх станів дозволяють значно покращити окремі криптографічні показники [14, 21 – 24]. Наприклад, за допомогою евристичних алгоритмів інформованого пошуку вдається значно підвищити нелінійність. Отже саме така генерація дозволяє досягти захищеності від більшості відомих атак: випадковість забезпечує високу алгебраїчну імунність, а евристичні техніки дозволяють покращити інші показники безпеки.

В цій роботі розглядаються евристичні техніки генерації вузлів заміни.

Для реалізації інформованого пошуку підходящого рішення в просторі можливих станів зазвичай застосовуються спеціальні евристичні функції (наприклад, у вигляді функції вартості) [25 – 27]. Евристична функція на кожному кроці на підставі додаткової інформації оцінює можливі альтернативи з метою прийняття рішення про те, в якому напрямку слід продовжувати пошук. При порівнянні можливих евристик мають значення ступінь інформованості (що визначається конкретною функцією вартості), а також складність обчислення кожної з евристик [25]. Більш поінформовані евристики дозволяють скоротити кількість вузлів пере-

борного пошуку, хоча платою за це можуть бути значні витрати часу на обчислення функції вартості для кожного вузла.

В роботі розглядається найбільш поширена версія функції вартості, що застосовується в більшості відомих евристичних алгоритмах генерації вузлів заміни. Метою дослідження є визначення конкретних параметрів евристичної функції, які з одного боку не знижують ступінь інформованості стосовно вузлів пошуку, а з іншого боку не вимагають значних обчислювальних витрат. Також надаються конкретні рекомендації з формування параметрів функції евристичного формування S-блоків.

Пов'язані роботи

Методи генерації криптографічних булевих функцій вивчалися в [10, 31, 37]. В роботах [6, 38] розглядаються векторні булеві функції для криптографічних застосувань. Зокрема, у [14, 23, 39 – 42] введено основні криптографічні показники S-блоків, вивчено їх властивості та досліджено різні техніки генерації.

Дослідженню евристичних методів пошуку нелінійних підстановок присвячено роботи [10, 11, 21, 34] та інші. Зокрема, у [28 – 30] досліджено інформований пошук локальних екстремумів, у роботах [14, 29, 31, 32] досліджено техніки градієнтного пошуку, роботи [12, 29, 33] присвячено алгоритмам імітації відпалу, в статтях [28, 34 – 36] розглянуто генетичні алгоритми і т.д.

Функції вартості досліджувалися в роботах [29, 33, 37, 39, 43] та ін. Зокрема, в [39, 43] досліджено алгоритми імітації відпалу, в [37] розглянуто метод «hill-climbing», в роботах [29, 33] досліджено різні функції вартості при їх застосуванні до різних технік евристичного пошуку.

В статті розглядаються та досліджуються найбільш поширені форми функції вартості з [39, 43] та досліджується вплив окремих показників на ефективність пошуку нелінійних вузлів заміни.

Вихідні дані та методика дослідження

В евристичному алгоритмі пошуку з використанням комбінаторної оптимізації користувач намагається вирішити проблему, створюючи або «розвиваючи» сутність певної форми [10, 11]. Спочатку користувач евристично визначає деяку цільову функцію («функцію вартості» або «функцію придатності»), яка приймає об'єкт, що еволюціонує, і видає скалярне значення. В алгоритмах, що використовують функції вартості, якісні рішення задач повинні відповідати низьким значенням цільової функції, а погані рішення – великим.

Метою комбінаторної оптимізації, до якої можна віднести ряд методів формування S-блоків зі заданими властивостями [29, 33, 44], завжди є мінімізація або максимізація певної цільової функції. Традиційно у алгоритмах імітації відпалу цільовою функцією називається функція вартості [39].

У 2000 р. було запропоновано нове сімейство функцій вартості, яке реалізувало суттєві покращення для випадку з одним виходом. Після значних експериментів ця функція вартості показала, що вона здатна створювати S-блоки з винятковими профілями критеріїв безпеки. Замість того, щоб засновувати вартість на екстремальних значеннях (згідно з визначенням нелінійності та автокореляції), вона визначила вартість у всьому спектрі Уолша – Адамара та спектрі автокореляції [39]. Деталі експериментів для окремого випадку випуску та детальна мотивація прийнятої функції вартості визначені у [43]. В цій статті застосовується та досліджується функція вартості у вигляді

$$WHS = \sum_{i=1}^{255} \left| \left| \max\left(WHT\right) \right| - X \right|^{R}, \qquad (1)$$

де X і R – дійсні параметри. У наявній літературі зазначається, що важко передбачити, якими повинні бути такі значення параметрів та з яких міркувань їх вибирати [29, 39, 43]. У цій

роботі досліджується поведінка функції вартості (1) та надаються відповідні рекомендації щодо вибору параметрів X і R.

Символ WHT (англ. Walsh – Hadamard transform) в (1) позначає спектральні коефіцієнти Уолша – Адамара. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації наведено на рис. 1 (тут і далі досліджуються бієктивні S-блоки із розміром входу-виходу 8*8).

У наведеному розподілі (рис. 1) максимальне є значення 68, середнє значення складає 49,2, а сума – 12 548. Якщо від всіх значень відняти 36, що буде відповідати параметру $X = 36$ з WHS, то гістограма набуде вигляду, який наведено на рис. 2. При цьому середнє значення буде складати 13,2, а сума – 3 368.

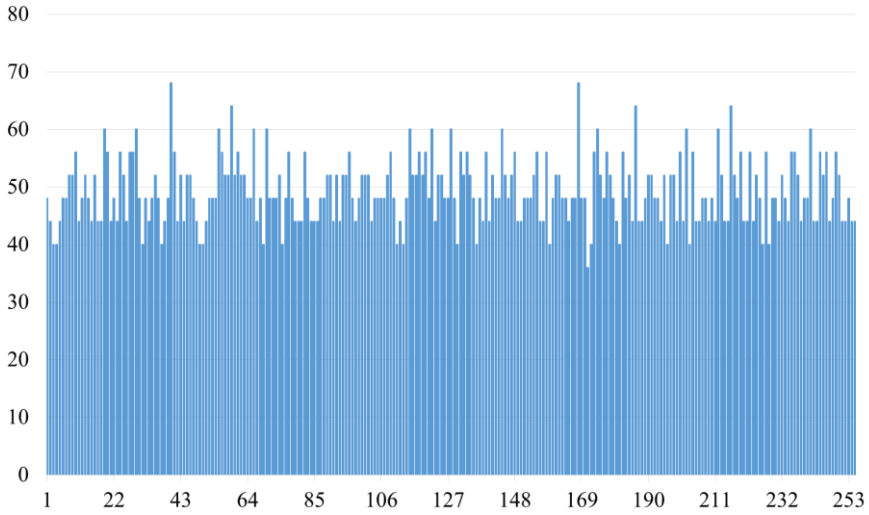


Рис. 1. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації

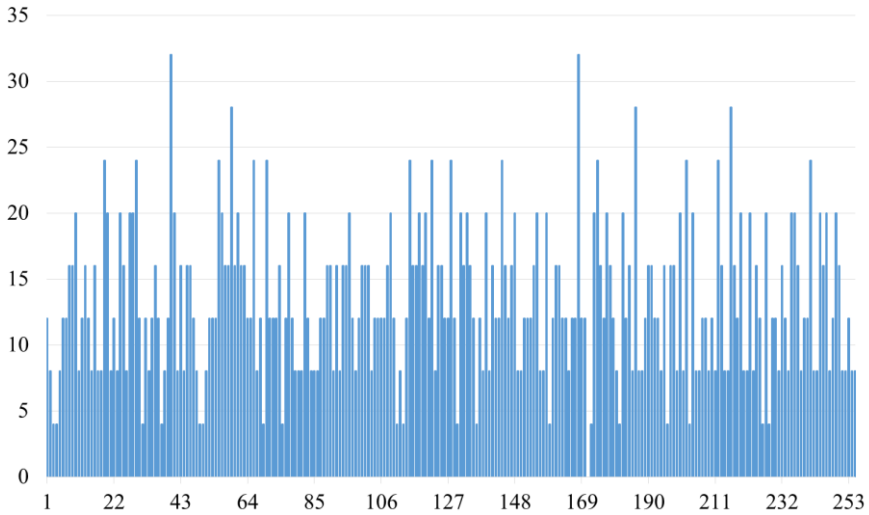


Рис. 2. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації з урахуванням параметру $X = 36$ з WHS

Максимальне значення спектру коефіцієнтів Уолша – Адамара ($\max(WHT)$) може приймати значення лише кратні чотирьом (детальніше це твердження розглянуто наприклад у [10, 11, 21]).

З метою експериментального встановлення розподілу, яке приймає WHS, було проведено серію окремих експериментів з різними вхідними параметрами X та R. Кожна серія складалась з 10^7 незалежних формувань випадковим чином S-блоку та встановлення його WHS.

Введемо наступні позначення:

- $f(WHS)$ – функція розподілу ймовірності значень WHS;
- $WHS^{\max}$ – значення функції розподілу ймовірності WHS при якому $f(WHS)$ приймає максимальне значення.

Окремо для кожної серії експериментів будемо підраховувати інтервал, до якого потрапляє 90 % найбільш значущих значень ймовірності $f(WHS)$. Величину значущості визначає $f(WHS)$. Інтервал підраховувався наступним чином:

1) до $f\left(WHS^{\max}\right)$ додавалося значення $f\left(WHS^{\max}+1\right)$ або $f\left(WHS^{\max}-1\right)$ в залежності від того, яке з них є більшим;
2) перевірялася сума;
3) якщо сума перевищувала 0,9, підрахунок вважалося завершеним, якщо ні – інтервал збільшувався на одиницю (в бік значення, яке було обрано в п.1) та процедура повторювалась знову.

Фіксувалась межа цього інтервалу:

- WHS^{-} – найменше значення функція розподілу ймовірності WHS, при якому $f(WHS)$ ще потрапляє до 90 % інтервалу найбільш значущих значень;
- WHS^{+} – найбільше значення функції розподілу ймовірності WHS, при якому $f(WHS)$ ще потрапляє до 90 % інтервалу найбільш значущих значень.

Метою цих досліджень є визначення впливу параметрів X і R на значення WHS та на ефективність евристичного пошуку.

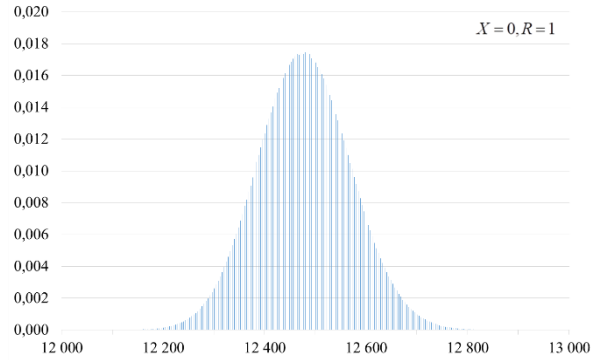
Отримані результати

Функції розподілу ймовірності значень WHS, які були отримані за результатами серії експериментів, наведено на рис. 3 – 7, у табл. 1 наведено основні показники, що характеризують функцію розподілу ймовірності та є вагомими.

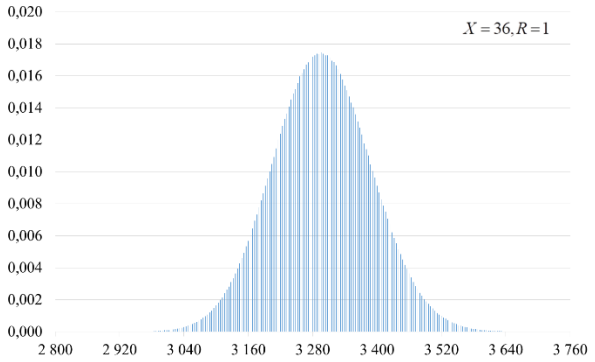
Таблиця 1

Результати дослідження WHS при різних параметрах R та X

R	X	$WHS^{\max}$	WHS^{-}	WHS^{+}	$f(WHS)$
1	0	12 480	12 324	12 632	рис. 3, *а*
1	22	6 862	6 714	7 022	
1	30	4 824	4 672	4 980	
1	35	3 548	3 396	3 704	
1	36	3 296	3 144	3 452	рис. 3, *б*
1	37	3 032	2 888	3 196	
1	38	2 784	2 636	2 944	
1	39	2 528	2 384	2 688	
1	40	2 280	2 132	2 436	
2	0	618 224	603 312	634 416	рис. 4, *а*
2	22	193 408	184 288	202 240	
2	36	50 880	46 144	55 808	рис. 4, *б*
3	0	31 144 000	29 896 000	32 352 000	рис. 5, *а*
3	22	5 664 000	5 216 000	6 112 000	
3	36	900 736	769 664	1 052 800	рис. 5, *б*
4	0	1 587 424 000	1 501 408 000	1 678 048 000	рис. 6, *а*
4	22	173 776 000	156 240 000	194 640 000	
4	36	17 735 680	14 110 720	22 917 120	рис. 6, *б*
5	0	81 184 000 000	75 616 000 000	87 552 000 000	рис. 7, *а*
5	22	5 587 200 000	4 800 000 000	6 547 200 000	
5	36	387 568 000	273 904 000	565 744 000	рис. 7, *б*

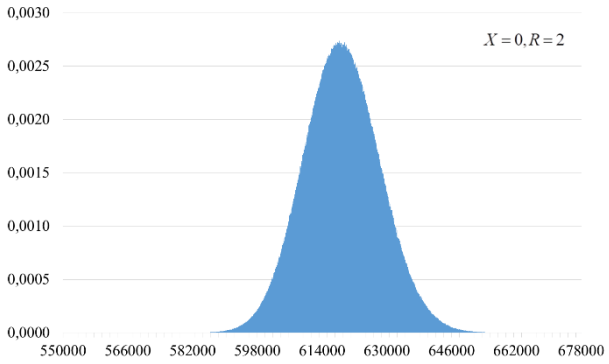


а

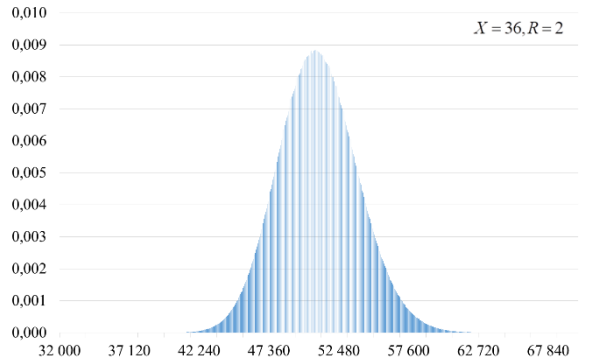


б

Рис. 3. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 1$ та *а* – $X = 0$, *б* - $X = 36$

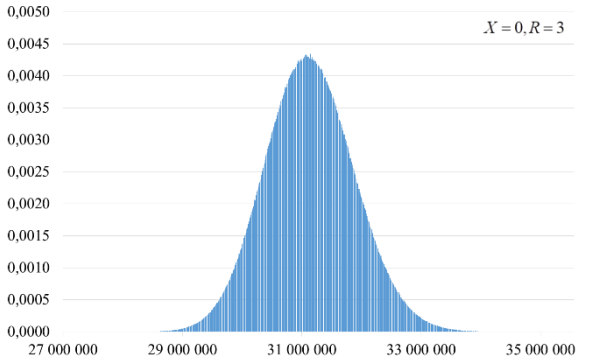


а

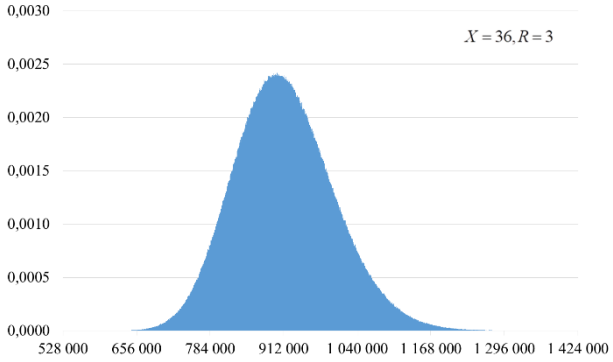


б

Рис. 4. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 2$ та *а* – $X = 0$, *б* – $X = 36$

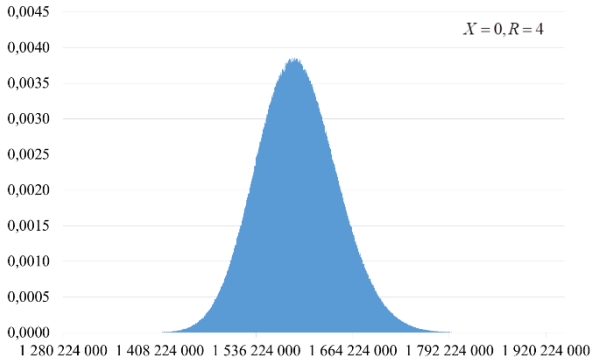


а

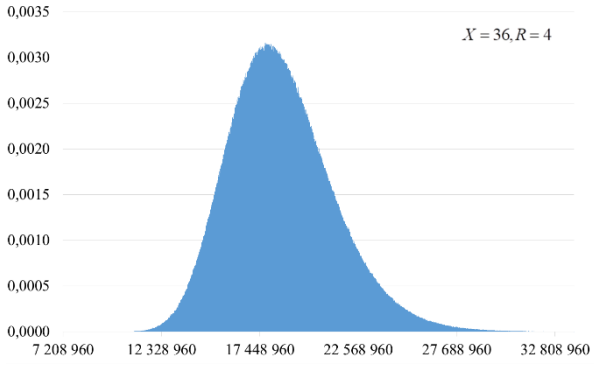


б

Рис. 5. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 3$ та *а* – $X = 0$, *б* – $X = 36$



а



б

Рис. 6. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 4$ та *а* – $X = 0$, *б* - $X = 36$

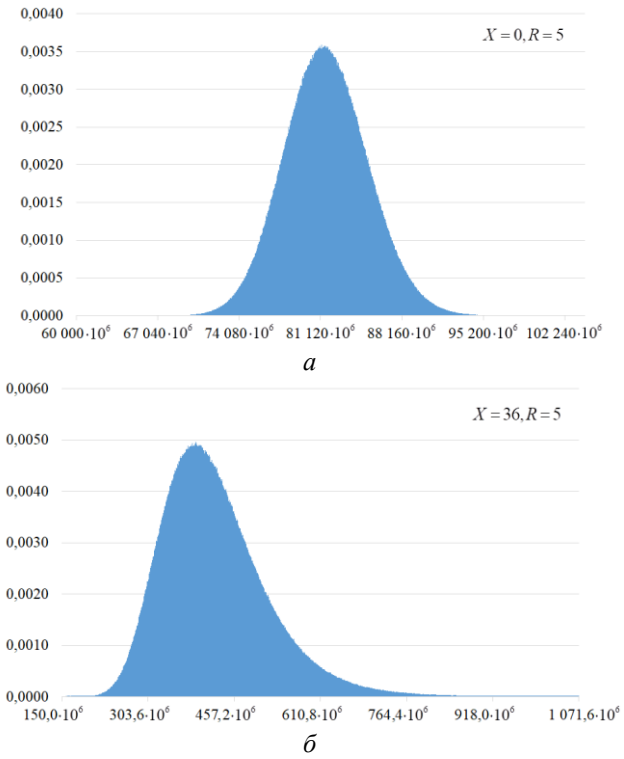


Рис. 7. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 5$ та *а* – $X = 0$, *б* - $X = 36$

З наведених результатів бачимо, що параметри X та R суттєво не впливають на форму функцій ймовірності розподілу самих значень. З ростом параметра R спостерігається невелика асиметрія, що пояснюється зведенням до степеню. Параметри можна вважати коефіцієнтами масштабування функції ймовірності розподілу *WHS*. Параметр R значно впливає на ширину функцій ймовірності розподілу цільової функції.

Змінюючи параметр X, можна переміщувати функцію ймовірності розподілу *WHS* по осі абсцис. Змінюючи значення X на одну одиницю, при $R = 1$, змінюємо значення *WHS* на 255 відповідно.

Збільшення параметру X призводить до наближення значень, які додаються у виразі (1), до нуля. Тому є сенс збільшувати цей параметр, що приведе до зменшення самих значень цільової функції з занадто великих значень до прийнятних.

Однак, якщо взяти параметр X великим, то завдяки модулю у виразі, при менших максимальних значень спектру Уолша – Адамара, вираз (1) буде мати більше значення *WHS*. Отже, при мінімізації значення *WHS* можливо спостерігати результат протилежну очікуваному.

Пояснимо останнє твердження, тобто якщо збільшувати параметр X, то при підсумовуванні максимальних значень спектру Уолша – Адамара за всіма 255 лінійними комбінаціями деякі з них можуть стати меншими за параметр X, що приведе до від'ємних значень. Але, завдяки модулю, сума абсолютних значень буде зростати, а з ним буде зростати значення *WHS*. Таким чином, якщо шукається S-блок з максимальною нелінійністю, а сума максимальних значень спектру Уолша – Адамара за всіма 255 лінійними комбінаціями буде менше за аналогічною сумою деякого попередньо найденого S-блоку (що потенційно може свідчить про більш високу нелінійність), то при великих значеннях параметр X, значення *WHS* буде вищим, а отже це буде вважатися за гірше рішення.

В якості прикладу такої поведінки *WHS* можна навести її функції ймовірності розподілу при різних параметрах X. На рис. 8 наведено результати дослідження розподілу $f(WHS)$ при

$R=1$ та зміни X від 0 до 70. Кожна серія складалась з 10^7 незалежних формувань випадковим чином S-блоку та встановлення його WHS.

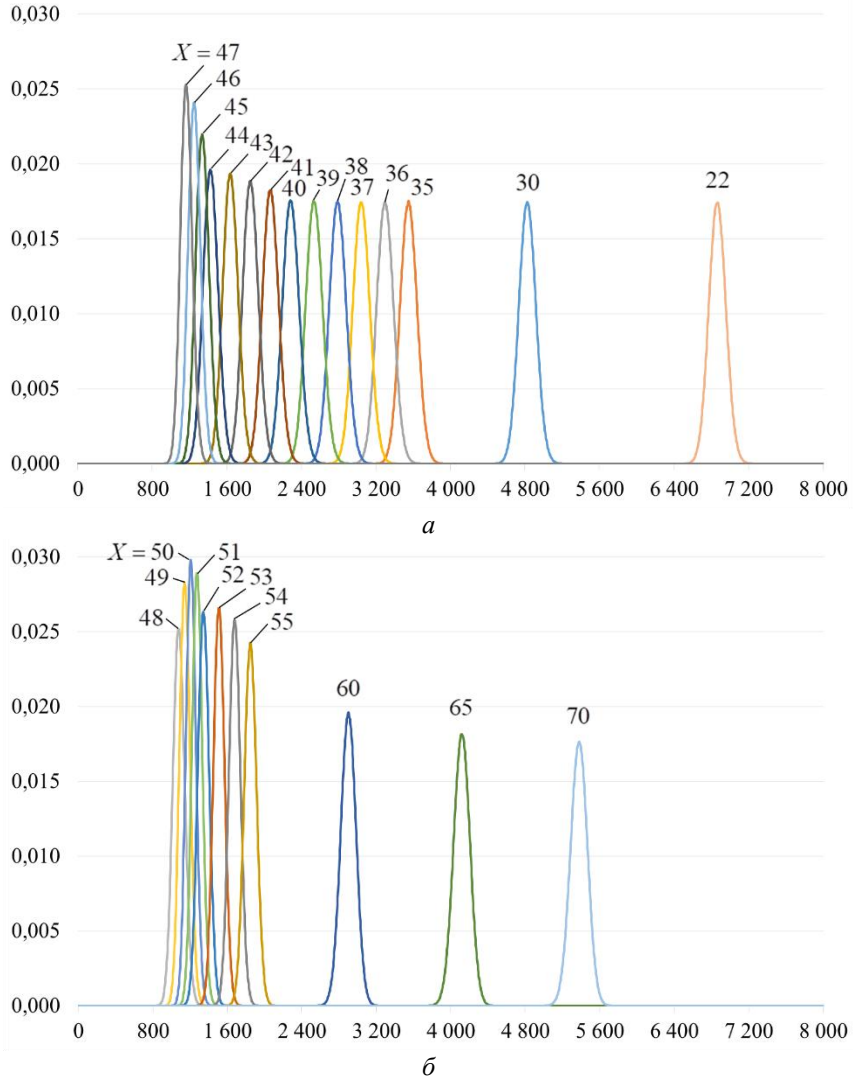


Рис. 8. $f(WHS)$ при $R=1$ та різних значеннях параметра X: *а* – $X=22-47$; *б* – $X=48-70$

Окремо, на рис. 9 наведено залежність $WHS^{\max}$ від параметру X, яку було встановлено при кожній серії. Пунктиром наведено розрахункове значення: $WHS^{\max}_{X=0}-255\cdot X$.

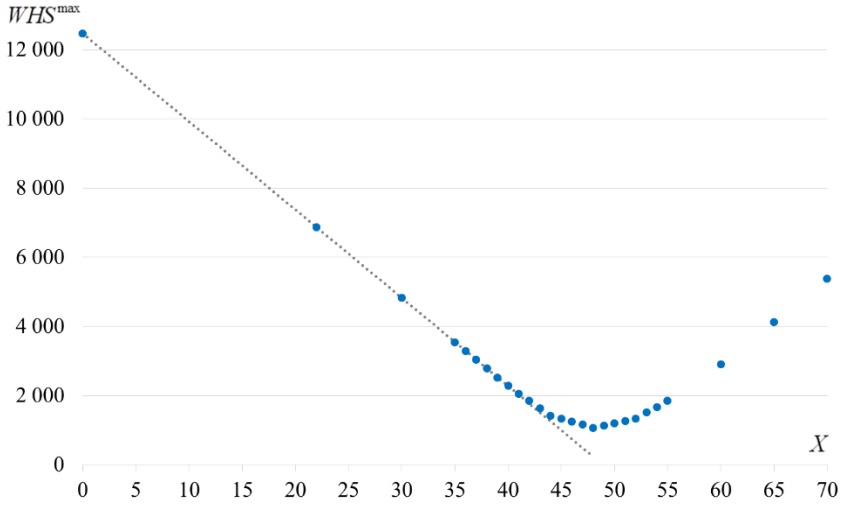


Рис. 9. $WHS^{\max}$ в залежності від параметру X при $R=1$

Значення WHS не знижується нижче деякого порогового значення (приблизно 1 000), яке відповідає сумі девіацій від середнього значення максимальних значень спектру Уолша – Адамара. Значне відхилення від розрахункового значення починається з порогового $X = 41$ (відхилення від розрахункового значення становить близько 2 %), а при $X = 44$ відхилення досягає 11,5 %, що свідчить о невідповідності поведінки WHS реальній картині та вже не може використовуватися в якості цільової функції. При застосуванні WHS на практиці є сенс його зменшення (без втрати адекватності відображення реальним значенням).

Зазначимо, що параметр R не впливає на величину знайденого порогового значення X, це випливає з безпосереднього аналізу виразу (1) для знаходження WHS. Порогове значення X зберігається при любих значеннях R.

При застосуванні на практиці величину $\left(WHS^{+} - WHS^{-}\right)$ є сенс збільшувати, що впливає на «чутливість» алгоритмів, які використовують WHS в якості цільових функції. Однак, при збільшенні параметру R значення WHS дуже швидко зростає та вже при $R = 5$ перевищує 32-бітне значення, що може негативно вплинути на швидкодію алгоритму та привести до небажаних помилок при застосуванні таких алгоритмів.

Висновки

Генерація нелінійних підстановок є важливим та актуальним напрямком пошукових досліджень, оскільки криптографічні параметри S-блоків безпосередньо впливають на стійкість симетричних шифрів до різних методів криптографічного аналізу (диференційного, лінійного, алгебраїчного та ін.). Найбільш перспективними вважаються евристичні техніки інформованого пошуку S-блоків, в яких застосовуються так звані функції вартості. Саме від властивостей цільових функцій та вибору їх окремих параметрів залежить ефективність евристичного пошуку, тобто конкретні обсяги часу та обчислювальних ресурсів, які витрачають для пошуку нелінійної підстановки із потрібними властивостями.

В роботі проаналізовано поведінку цільової функції (1), яка використовується в алгоритмах формуваннях S-блоків із заданими криптографічними властивостями (наприклад, локального пошуку, градієнтного підйому, імітації відпалу, генетичного пошуку, тощо). Також в роботі надано рекомендації з вибору параметрів зазначеної функції.

В якості оптимальних параметрів цільової функції (1) обрано:

- $X = 36$ як максимально допустиме значення, яке зменшує WHS, але не приводить до суттєвого впливу на її адекватний взаємозв'язок з нелінійністю S-блоку;
- $R = 4$ як максимально допустиме значення, яке збільшує діапазон можливих значень WHS, що може покращити «чутливість» алгоритмів формування S-блоків, які її використовують.

Зазначені параметри доцільно використовувати в різних алгоритмах евристичного пошуку. Це дозволить, на нашу думку, значно підвищити ефективність генерації нелінійних підстановок.

References:

1. Menezes A.J., Oorscho, P.C., van Vanstone S.A., Oorschot P.C. van, Vanstone S.A. Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
2. Schneier B. Applied cryptography : protocols, algorithms, and source code in C. New York : Wiley (1996).
3. Technology N.I. of S. and: Advanced Encryption Standard (AES). U.S. Department of Commerce (2001). https://doi.org/10.6028/NIST.FIPS.197.
4. Kuznetsov A., Gorbenko Y., Andrushkevych A., Belozersev I. Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2 // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). pp. 203–206 (2017). https://doi.org/10.1109/INFOCOMMST.2017.8246380.
5. Kuznetsov O., Potii O., Perepelitsyn A., Ivanenko D., Poluyanenko N. Lightweight Stream Ciphers for Green IT Engineering // Kharchenko V., Kondratenko Y., and Kacprzyk J. (eds.) Green IT Engineering: Social, Business and Industrial Applications. pp. 113–137. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-00253-4_6.

6. Álvarez-Cubero J. Vector Boolean Functions: applications in symmetric cryptography (2015). https://doi.org/10.13140/RG.2.2.12540.23685.

7. AlSalami Y., Martin T., Yeun C. Linear and Differential Properties of Randomly Generated DES-Like Substitution Boxes // Park, J.J. (Jong H., Stojmenovic I., Jeong H.Y., and Yi G. (eds.) Computer Science and its Applications. pp. 517–524. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-45402-2_77.

8. Eastlake 3rd D., Schiller J., Crocker S. Randomness Requirements for Security. (2005).

9. Daemen J., Rijmen V. Specification of Rijndael // Daemen, J. and Rijmen, V. (eds.). The Design of Rijndael: The Advanced Encryption Standard (AES). pp. 31–51. Springer, Berlin, Heidelberg (2020). https://doi.org/10.1007/978-3-662-60769-5_3.

10. Burnett L.D. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography, https://eprints.qut.edu.au/16023/ (2005).

11. Clark A.J. Optimisation heuristics for cryptology, https://eprints.qut.edu.au/15777/, (1998).

12. Clark J.A., Jacob J.L., Stepney S. The design of s-boxes by simulated annealing. In: Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1533-1537 Vol. 2 (2004). https://doi.org/10.1109/CEC.2004.1331078.

13. Nyberg K. Linear Approximation of Block Ciphers. In: EUROCRYPT (1994). https://doi.org/10.1007/BFb0053460.

14. Millan W. How to improve the nonlinearity of bijective S-boxes. In: Boyd, C. and Dawson, E. (eds.). Information Security and Privacy. pp. 181–192. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0053732.

15. Nover H. Algebraic Cryptanalysis of Aes: An Overview.

16. Bard G.V. Algebraic Cryptanalysis. Springer US, Boston, MA (2009). https://doi.org/10.1007/978-0-387-88757-9.

17. Ferguson N., Schroeppel R., Whiting D. A Simple Algebraic Representation of Rijndael // Vaudenay S. and Youssef A.M. (eds.). Selected Areas in Cryptography. pp. 103–111. Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/3-540-45537-X_8.

18. Courtois N.T., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // Zheng, Y. (ed.) Advances in Cryptology – ASIACRYPT 2002. pp. 267–287. Springer, Berlin, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_17.

19. Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Galbraith, S.D. (ed.). Cryptography and Coding. pp. 152–169. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77272-9_10.

20. Kuznetsov O.O., Gorbenko Y.I., Bilozertsev I.M., Andrushkevych A.V., Narizhnyi O.P.: ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. TRE. 77, (2018). https://doi.org/10.1615/TelecomRadEng.v77.i4.30.

21. Millan W., Burnett L., Carter G., Clark A., Dawson E. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes // Varadharajan V. and Mu Y. (eds.) Information and Communication Security. pp. 263–274. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/978-3-540-47942-0_22.

22. Nedjah N., Mourelle L. de M., Mourelle L. de M. Multi-objective Evolutionary Design of Robust Substitution Boxes, https://www.taylorfrancis.com/, last accessed 2020/07/25. https://doi.org/10.1201/9781315366845-7.

23. Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the High Nonlinear S-Boxes Generation Method. Tatra Mountains Mathematical Publications. 70, 93–105 (2017). https://doi.org/10.1515/tmmp-2017-0020.

24. Laskari E.C., Meletiou G.C., Vrahatis M.N. Utilizing Evolutionary Computation Methods for the Design of S-Boxes. In: 2006 International Conference on Computational Intelligence and Security. pp. 1299–1302 (2006). https://doi.org/10.1109/ICCIAS.2006.295267.

25. Edelkamp S., Schroedl S. Heuristic Search Theory and Applications. Morgan Kaufmann, Amsterdam ; Boston (2011).

26. Informed Search Algorithms in AI – Javatpoint, https://www.javatpoint.com/ai-informed-search-algorithms, last accessed 2021/05/19.

27. Katz M., Domshlak C. Optimal admissible composition of abstraction heuristics. Artificial Intelligence. 174, 767–798 (2010). https://doi.org/10.1016/j.artint.2010.04.021.

28. Kapuściński T., Nowicki R.K., Napoli C. Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes // Rutkowski L., Korytkowski M., Scherer R., Tadeusiewicz R., Zadeh L.A., and Zurada J.M. (eds.) Artificial Intelligence and Soft Computing. pp. 380–391. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-39378-0_33.

29. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes. Evolutionary Computation. 24, 695–718 (2016). https://doi.org/10.1162/EVCO_a_00191.

30. Cusick T., Stănică P. Cryptographic Boolean Functions and Applications: Second edition. (2017).

31. Izbenko Y., Kovtun V., Kuznetsov A. The Design of Boolean Functions by Modified Hill Climbing Method // 2009 Sixth International Conference on Information Technology: New Generations. pp. 356–361. IEEE, Las Vegas, NV, USA (2009). https://doi.org/10.1109/ITNG.2009.102.

32. Freyre-Echevarría A., Martínez-Díaz I., Pérez C.M.L., Sosa-Gómez G., Rojas O. Evolving Nonlinear S-Boxes With Improved Theoretical Resilience to Power Attacks // IEEE Access. 8, 202728–202737 (2020). https://doi.org/10.1109/ACCESS.2020.3035163.

33. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. (2020).

34. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 8, 247–276 (2016). https://doi.org/10.1007/s12095-015-0170-5.

35. Freyre-Echevarría A., Alanezi A., Martínez-Díaz I., Ahmad M., Abd El-Latif A.A., Kolivand H., Razaq A. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes // Symmetry. 12, 1896 (2020). https://doi.org/10.3390/sym12111896.

36. Tesar P. A New Method for Generating High Non-linearity S-Boxes (2010).

37. Kavut S., Yücel M.D. Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria // Johansson, T. and Maitra, S. (eds.) Progress in Cryptology – INDOCRYPT 2003. pp. 121–134. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24582-7_9.

38. Carlet C. Vectorial Boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering (2006).

39. Clark J.A., Jacob J.L., Stepney S. The design of S-boxes by simulated annealing // New Gener Comput. 23, 219–231 (2005). https://doi.org/10.1007/BF03037656.

40. Nyberg K. Perfect nonlinear S-boxes // Davies, D.W. (ed.) Advances in Cryptology — EUROCRYPT ’91. pp. 378–386. Springer, Berlin, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_32.

41. Carlet C., Ding C. Nonlinearities of S-boxes. Finite Fields and Their Applications. 13, 121–135 (2007). https://doi.org/10.1016/j.ffa.2005.07.003.

42. Fuller J., Millan W. Linear Redundancy in S-Boxes // Johansson, T. (ed.) Fast Software Encryption. pp. 74–86. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39887-5_7.

43. Clark J.A., Jacob J.L., Stepney S. Searching for cost functions // Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1517-1524 Vol.2 (2004). https://doi.org/10.1109/CEC.2004.1331076.

44. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Pasalic, E. and Knudsen, L.R. (eds.) Cryptography and Information Security in the Balkans. pp. 31–42. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3.

Надійшла до редколегії 12.09.2021

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Катрич Віктор Олександрович – д-р фіз.-мат. наук, професор, заслужений діяч науки і техніки України, Харківський національний університет імені В.Н. Каразіна, проректор з наукової робот; Україна; e-mail: vkatrich@karazin.ua, ORCID: https://orcid.org/0000-0001-5429-6124

Кандій Сергій Олегович – технік-конструктор, АТ «Інститут інформаційних технологій», Україна; e-mail: sergeykandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

Заїченко Юлія Олександрівна – магістрант, Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: yuliya.zaicenko.00@gmail.com, ORCID: https://orcid.org/0000-0001-6116-2693